



Sicherheit am Strand

# Netzwerksicherheit

— Risiken und Schutzmöglichkeiten —

Prof. Dr. Hannes Federrath

Universität Regensburg

Lehrstuhl Management der Informationssicherheit

<http://www-sec.uni-regensburg.de/>

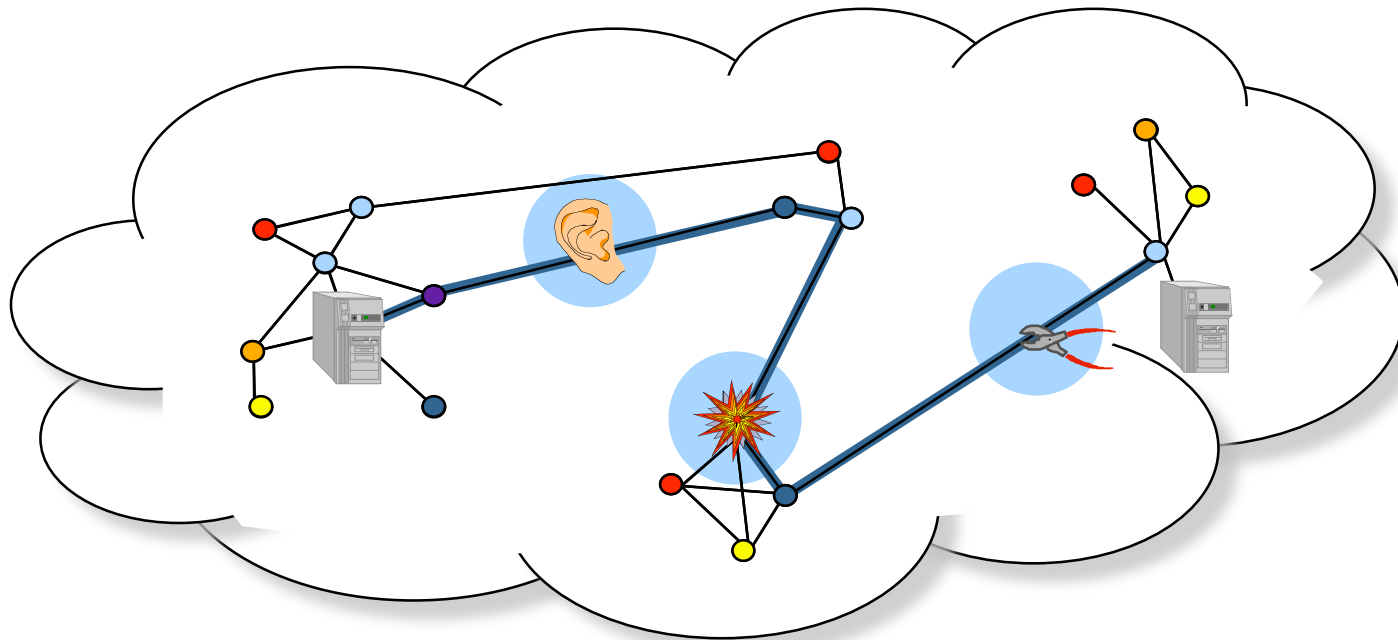
## Gliederung

- Einordnung
  - Netzwerksicherheit – Rechnersicherheit
  - Schutzziele
- Angriffe: Fallbeispiele
  - Viren, Würmer, trojanische Pferde
  - Phishing
  - Sniffing und Spoofing



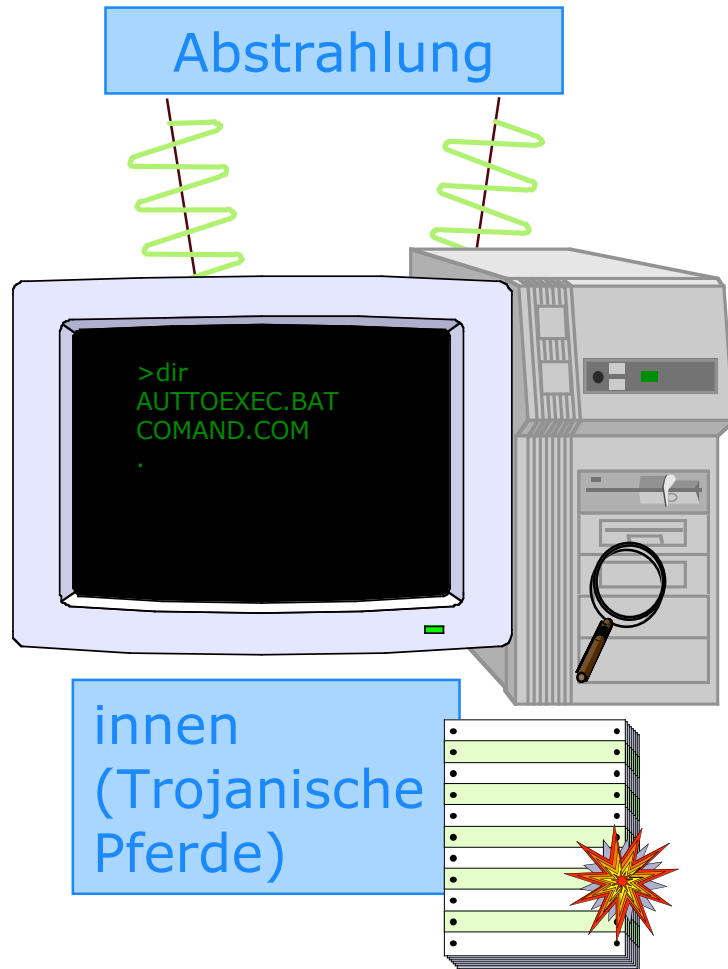
## Netzwerksicherheit – Rechnersicherheit

- Knoten: Rechner
- Kanten: Übertragungsstrecken

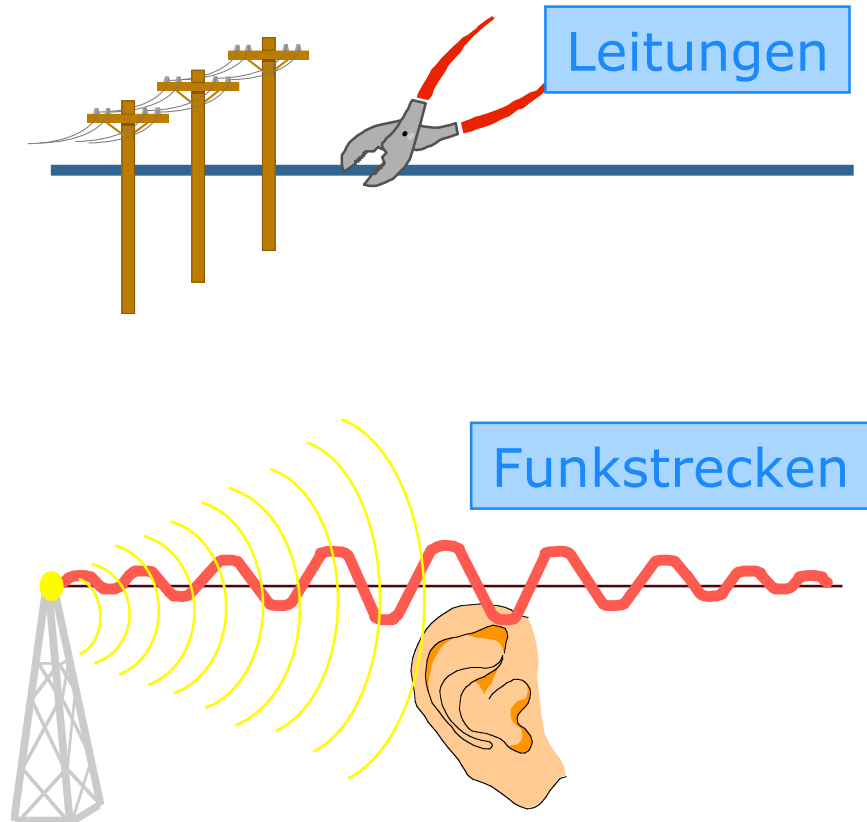


# Angriffspunkte

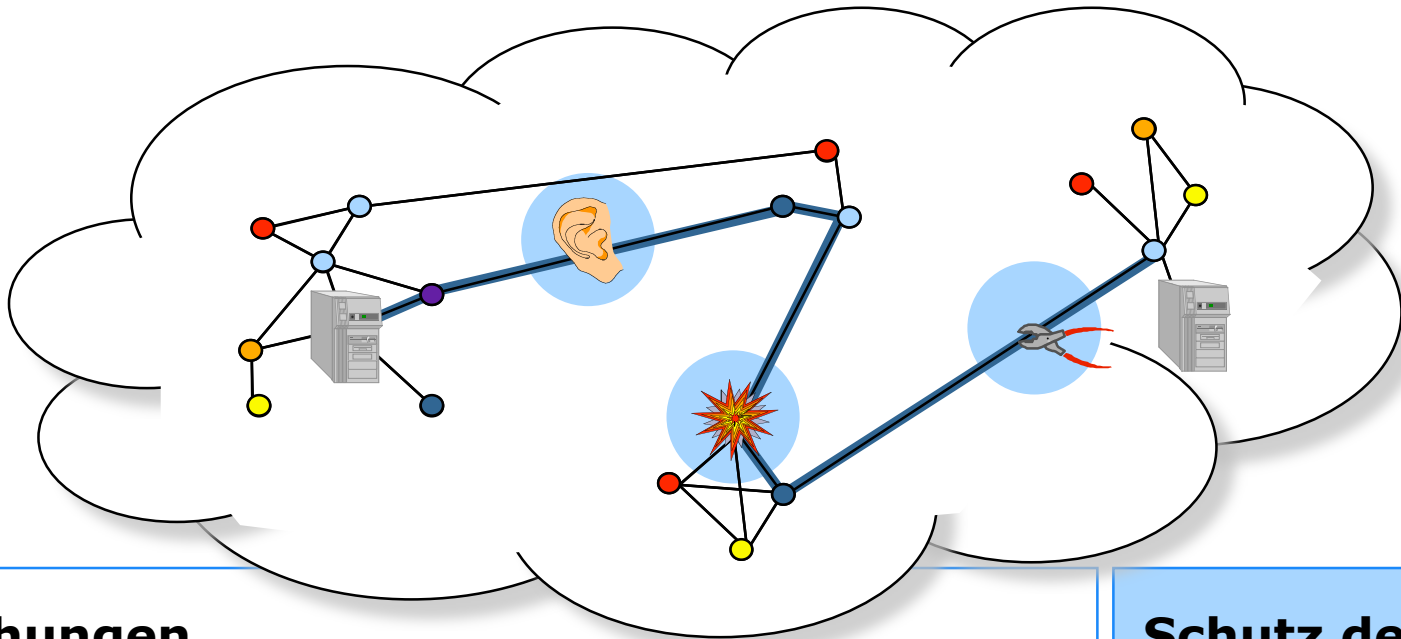
## Rechnersicherheit



## Netzwerksicherheit



# Sicherheit in Rechnernetzen



## Bedrohungen



unbefugter Informationsgewinn



unbefugte Modifikation



unbefugte Beeinträchtigung der Funktionalität

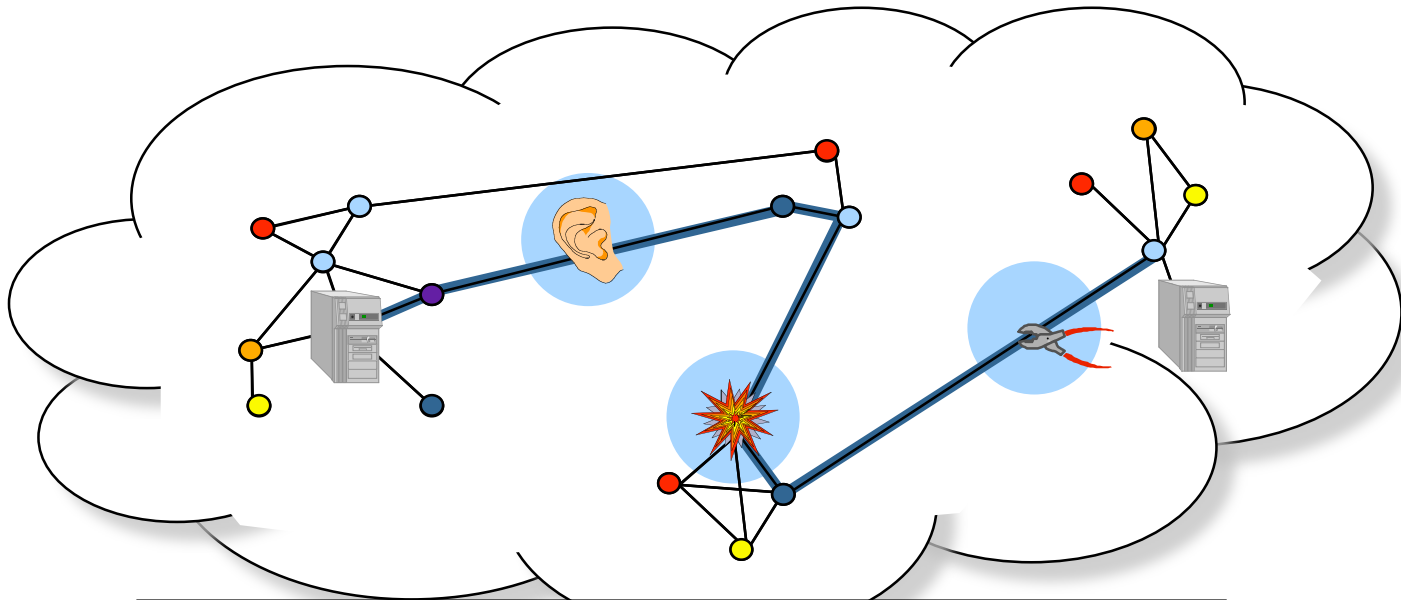
## Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

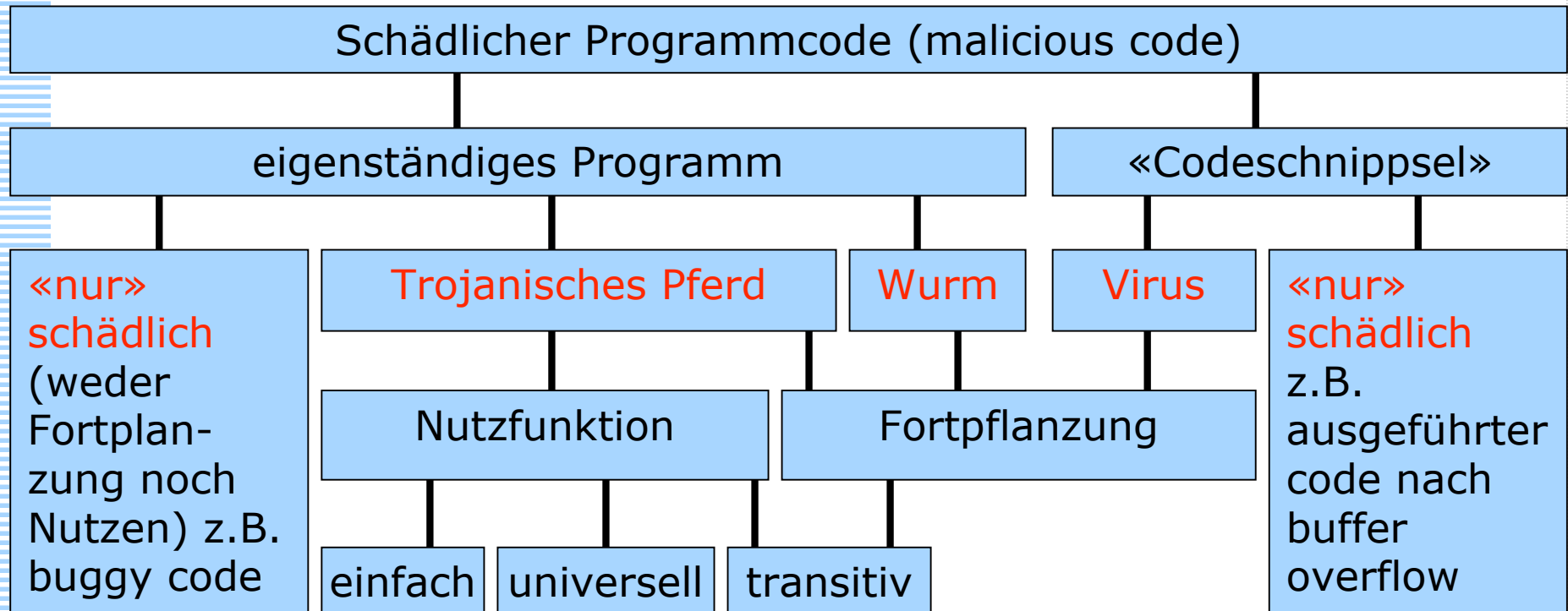
## Angriffe: Fallbeispiele



V: Viren, Würmer, trojanische Pferde

P: Phishing

S: Sniffing und Spoofing



# Trojanische Pferde

Newsletter Ausgabe vom 09.06.2005

<http://www.bsi-fuer-buerger.de/newsletter/newsletter> Unfairer Wettbewerb: Spionage

über das BSI | Fragen? | Ihre Meinung | Impressum

**Ins Internet**

- <http://n-tv.de/537669.html>
- <http://www.winboard.org/lofiversion/index.php/t30390.html>
- <http://www.pcwelt.de/news/sicherheit/112831/index.html>
- <http://www.bsi-fuer-buerger.de/newsletter/newsletter05/newsletter090605.htm>

**SICHER • INFORMIERT**

Der Newsletter von  
www.bsi-fuer-buerger.de  
Ausgabe vom 09.06.2005

**Unfairer Wettbewerb: Spionage-Krimi um Trojanisches Pferd**

Computerviren als Waffen im Kampf um wirtschaftliche Macht - das ist keine Zukunftsvision, sondern offensichtlich bereits Realität. In Israel wurden in einer groß angelegten Aktion insgesamt 18 Verdächtige verhaftet, die mit Hilfe eines Trojanischen Pferdes Industriespionage betrieben haben sollen. Das Schadprogramm, das ein in Großbritannien und Deutschland lebender Programmierer entwickelt haben soll, wurde angeblich in Konkurrenzunternehmen eingeschleust. Dort habe es dann, so die Vorwürfe, sensible Daten ausgespäht und an die Betrüger übermittelt.

Dieser Newsletter ist ein kostenloses Service-Angebot des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de. Er erscheint im Abstand von 14 Tagen. Die Informationen werden mit größter Sorgfalt recherchiert und aufbereitet, dennoch kann eine Gewähr oder Haftung für die Vollständigkeit und Richtigkeit nicht übernommen werden.

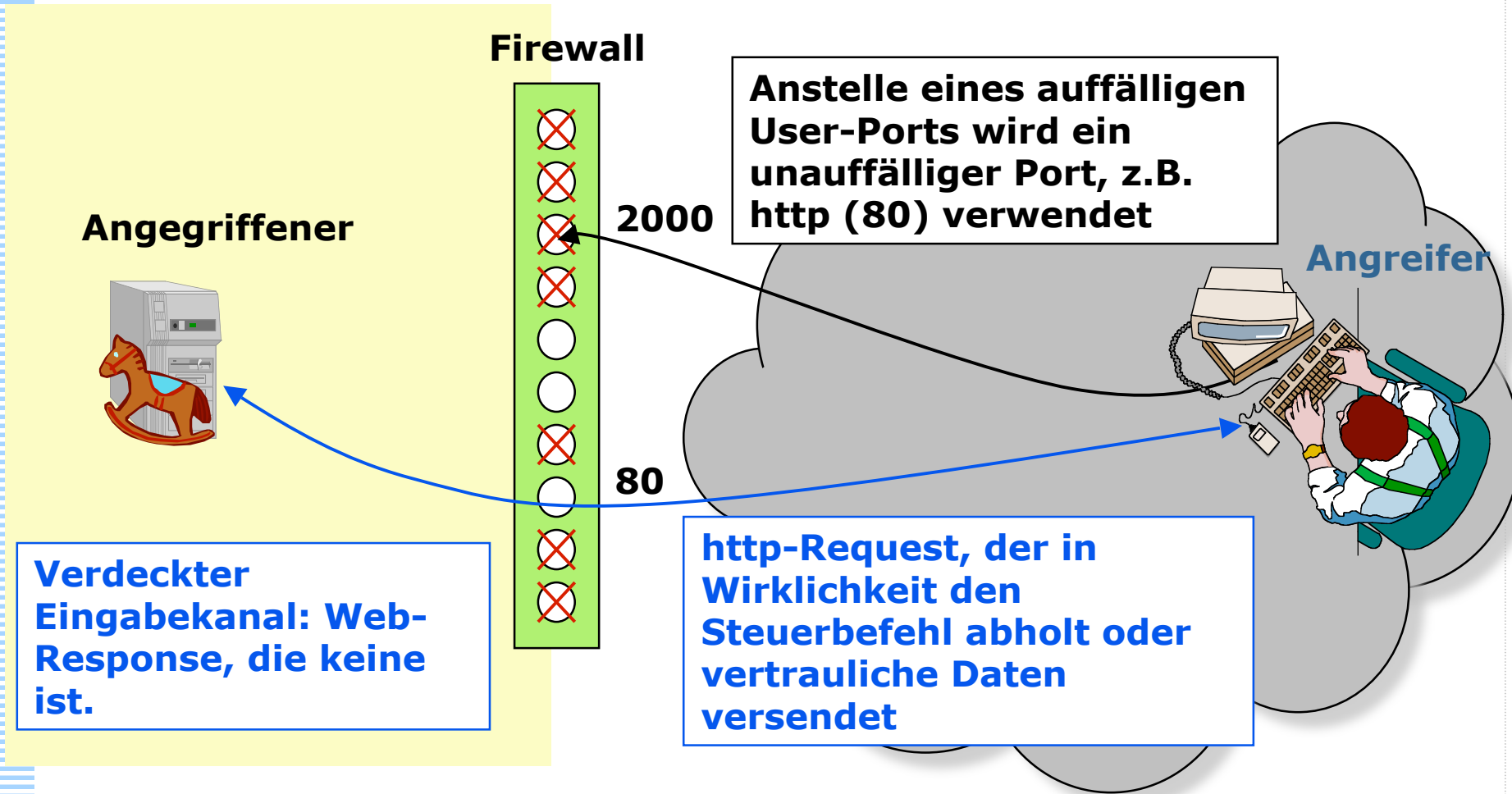
**IT-Sicherheit**

- Das Internet
- Der Browser
- Datensicherung
- Viren & andere Tiere
- Abzocker & Spione
- Infiziert - und nun?
- Schützen - aber wie?
- Themen

gezielter Einsatz statt  
Massenverbreitung

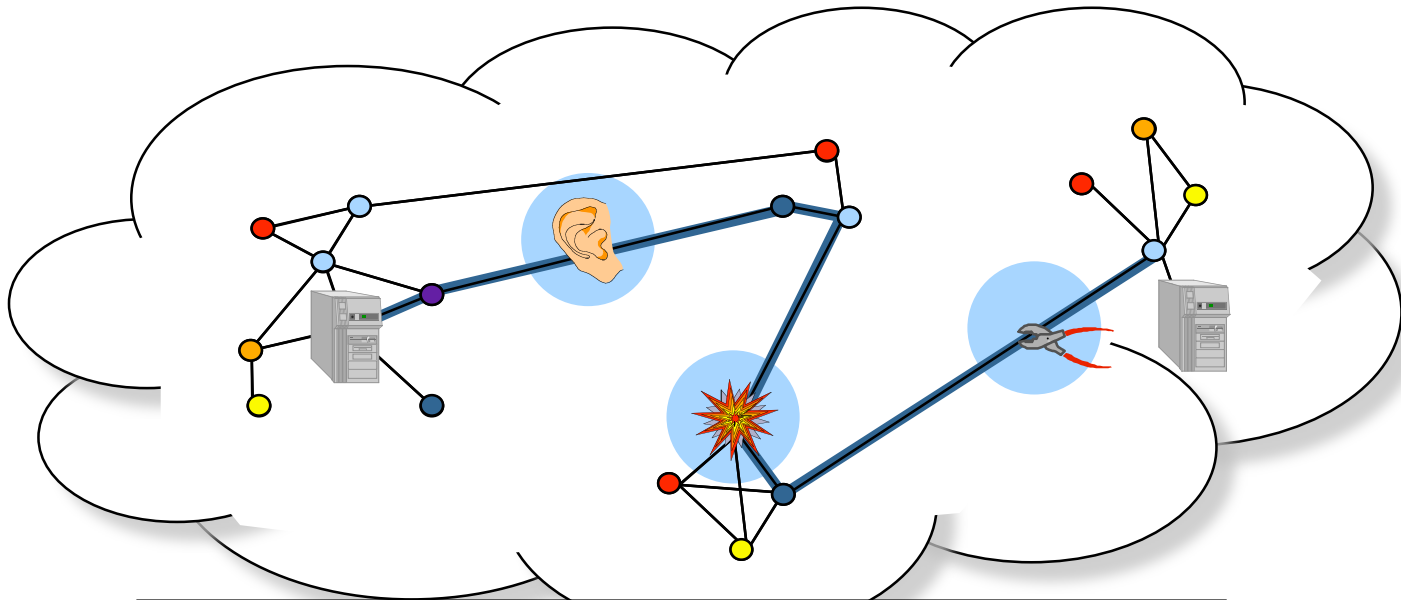


# Untertunneln einer Firewall durch Troj. Pferd



➡ Firewall verhindert nicht die Wirkung des trojanischen Pferdes

## Angriffe: Fallbeispiele



V: Viren, Würmer, trojanische Pferde

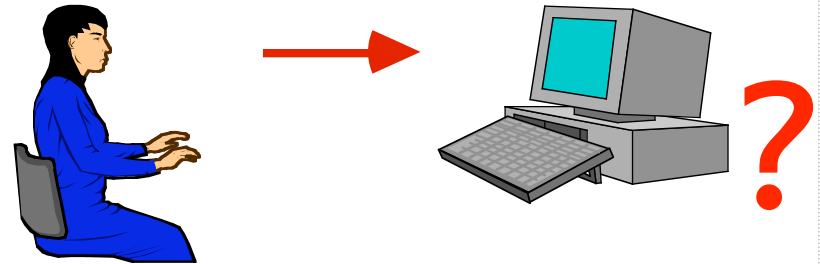
P: Phishing

S: Sniffing und Spoofing

# Identifikation von Menschen durch IT-Systeme

## • Was der MENSCH IST:

- Handgeometrie
- Fingerabdruck
- **Aussehen\***
- **eigenhändige Unterschrift\***
- Retina-Muster
- Stimme
- Tipp-Charakteristik
- DNA-Muster



## • Was der MENSCH HAT:

- **Papierdokument\***
- Metallschlüssel
- Magnetstreifenkarte
- Chipkarte
- Taschenrechner



Bild:  
<http://www.rsasecurity.com>

## • Was der MENSCH WEIß:

- Passwort
- Antworten auf Fragen
- Rechenergebnisse für Zahlen

**\*=Ausweis**



Bild: ntz, Heft 3-4/2006, S. 35

## Welche Passwörter werden tatsächlich genutzt?

- Kompromittierte Passwörter eines Internet-Dating-Portals wurden auf einer Mailingliste veröffentlicht:
  - Ein blinder Log-in-Versuch mit "123456" führt in fast 1,4 % der Fälle zum Erfolg.
  - Insgesamt rund 2,5 % der Passwörter beginnen mit der Ziffernfolge "1234".
  - Rund 40 % der Passwörter trat nur einmal auf.

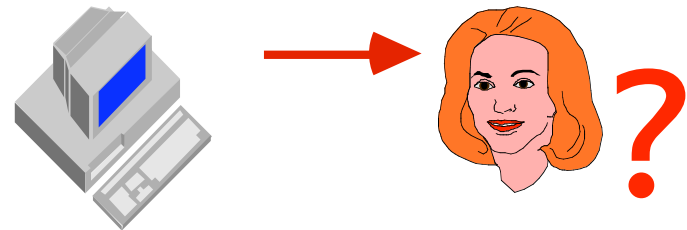
Rang	Passwort	Häufigkeit
1	123456	1375
2	ficken	404
3	12345	367
4	hallo	362
5	123456789	260
6	schatz	253
7	12345678	215
8	daniel	215
9	askim	184
10	nadine	177
11	1234	176
12	passwort	173

... Quelle: ct 2006, Heft 13, S.64

## Identifikation von IT-Systemen durch Menschen

- Was es ist:

- Gehäuse
- Siegel
- Hologramm
- Verschmutzung



- Was es weiß:

- Passwort
- Antworten auf Fragen
- Rechenergebnisse für Zahlen

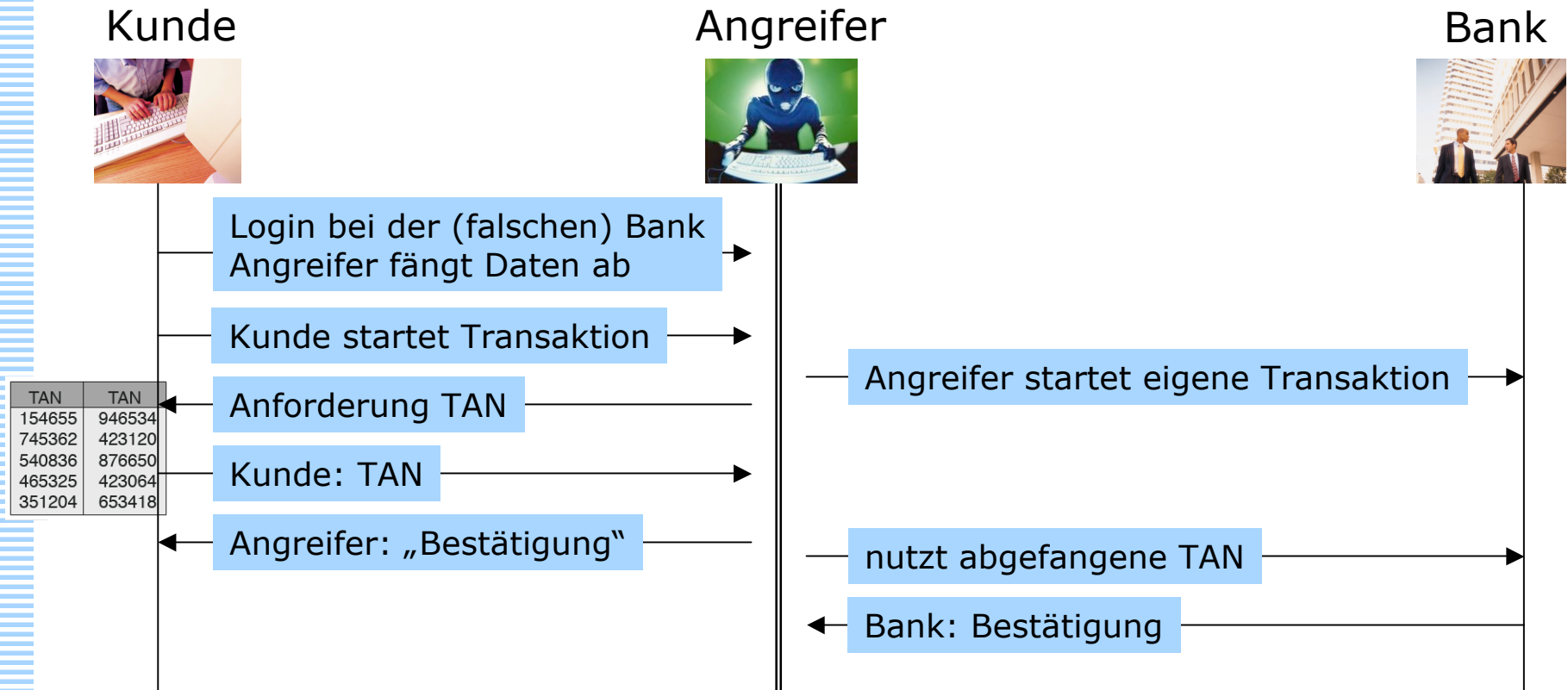
Warum ist das relevant?

- Faked Login-Screen
- Phishing

- Wo es steht.

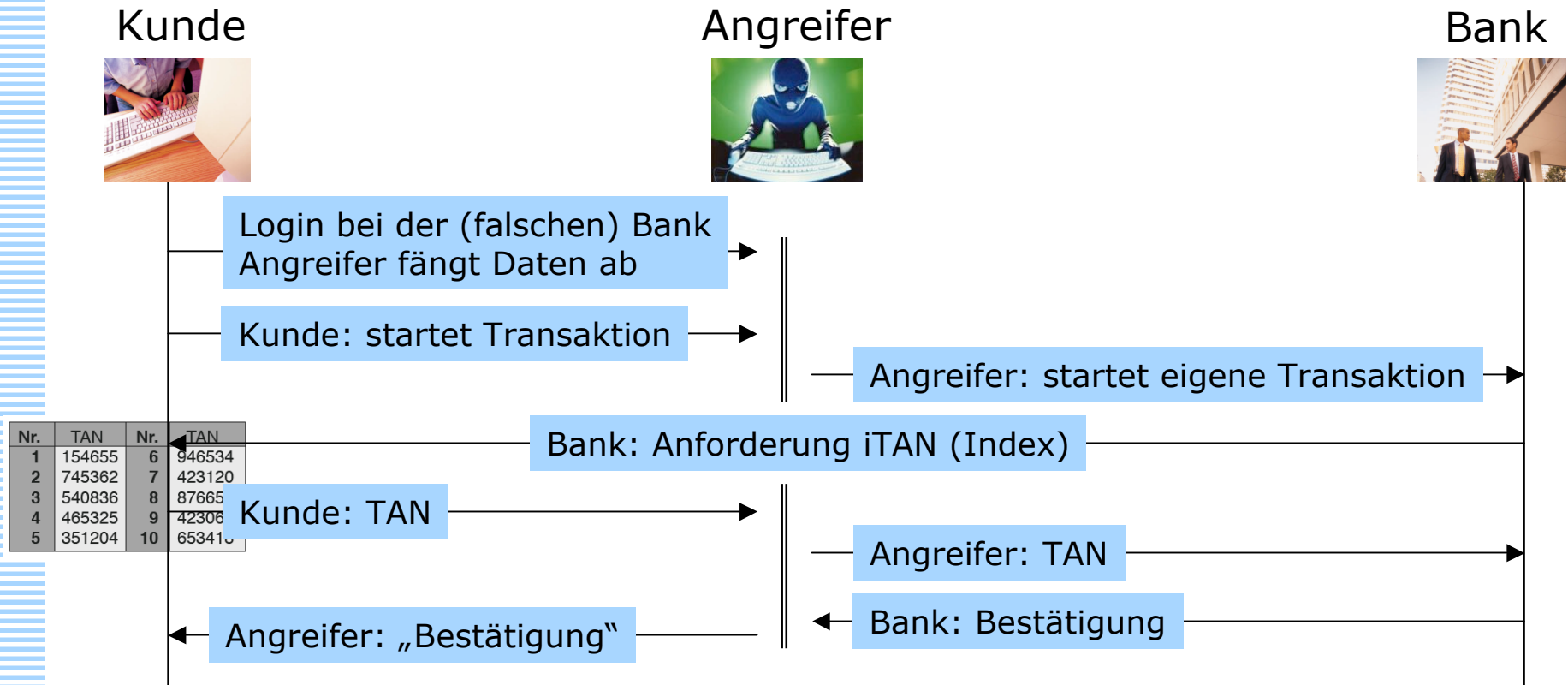
## Man-in-the-middle-attack auf TAN-Verfahren (Skizze)

- **Voraussetzung: Angreifer**
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite



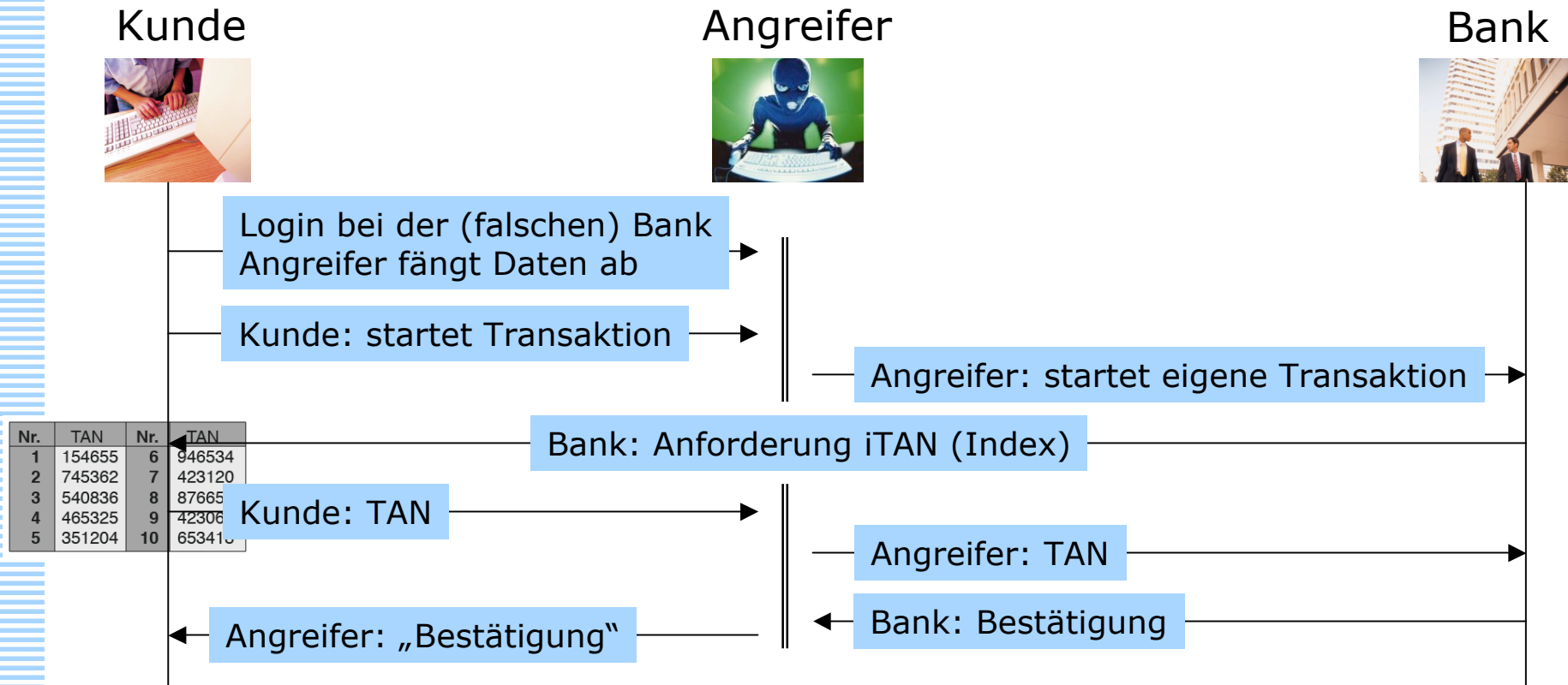
## Man-in-the-middle-attack auf iTAN-Verfahren (Skizze)

- **Voraussetzung: Angreifer**
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite



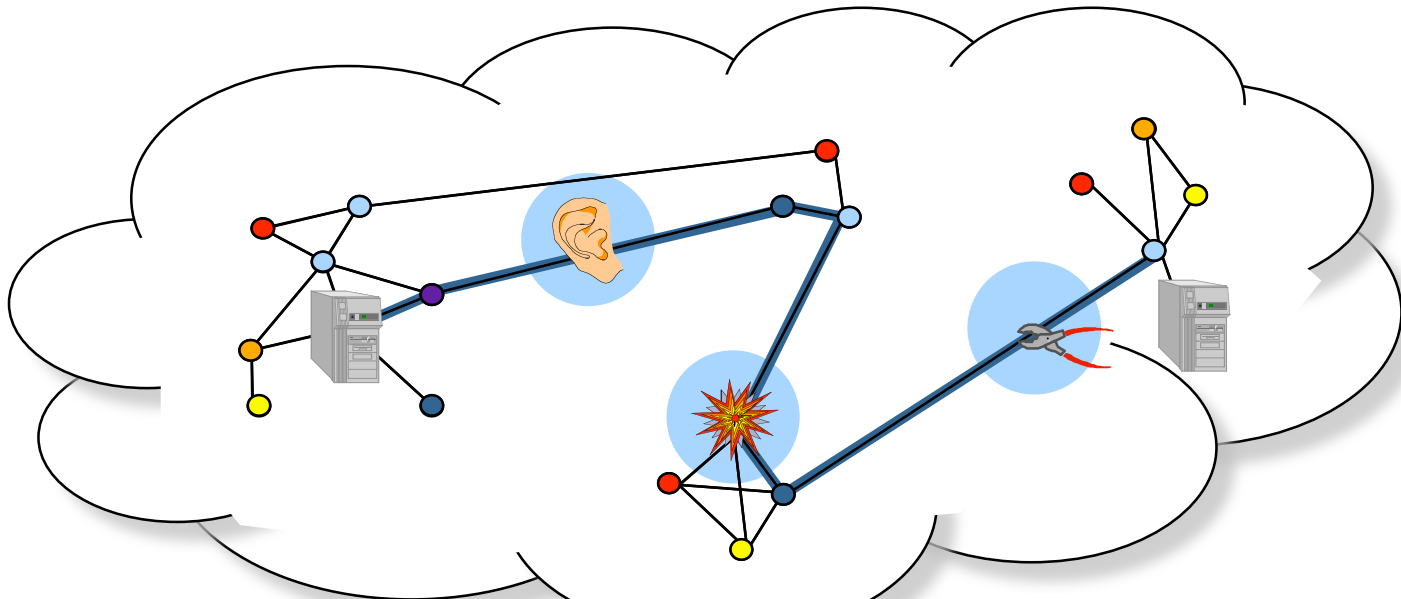
## Man-in-the-middle-attack auf iTAN-Verfahren (Skizze)

- Verbesserungen gegenüber normalem TAN-Verfahren:
  - Angreifer benötigt «Online-Hilfe durch Kunden», d.h. er kann nur Transaktionen erfolgreich durchführen, wenn Kunde dies selbst gerade tun will





## Angriffe: Fallbeispiele



V: Viren, Würmer, trojanische Pferde

P: Phishing

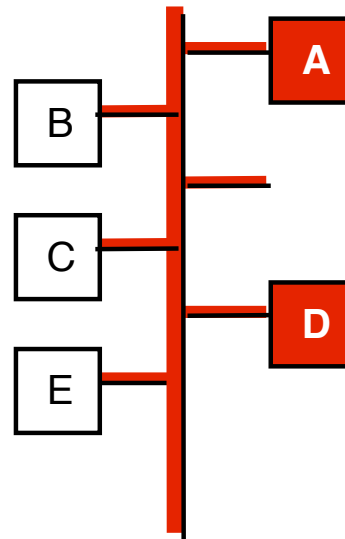
S: Sniffing und Spoofing

## Sniffing-Angriffe: Funktionsweise (Ethernet)

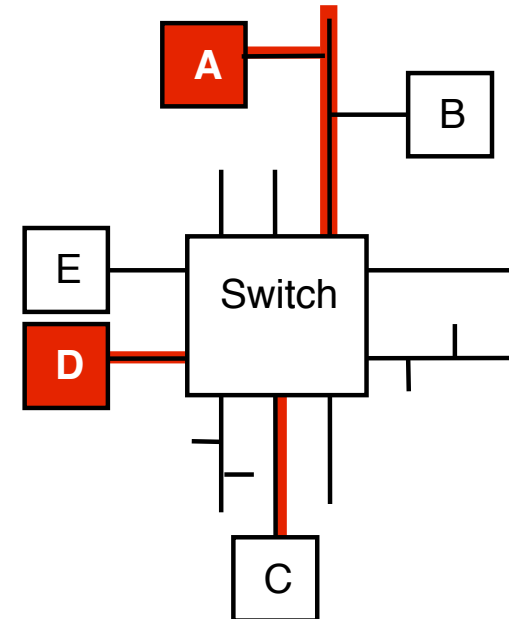
- alle Stationen erhalten alle Datenpakete (im Ethernet)
- lokale Filterfunktion
- Abschalten des Filters möglich:  
»**promiscuous mode**«
- Sniffing im Switched Ethernet erschwert

Rechner **A** und **D** kommunizieren miteinander:

a) im Ethernet



b) im Switched Ethernet



Ausbreitung der übertragenen Daten

## Sniffing-Angriffe: Vorgehen

- 1. Schritt – Beschaffung der Daten
  - Konfiguration der Netzwerkschnittstelle (promiscuous mode)
  - Auslesen sämtlicher Datenpakete
- 2. Schritt – Informationsgewinnung
  - Auswahl der »interessanten« Pakete anhand der Protokoll-Informationen (Sender- bzw. Empfängeradresse, TCP-Port etc.)
- 3. Schritt – Auswertung des Datenteils



```
/usr/bin/login (ttyp1)
11:47:15.106002 titanus.inf.fu-berlin.de.49615 > www.linux.org
11:47:15.171156 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.220038 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.220170 titanus.inf.fu-berlin.de.49616 > www.linux.org
11:47:15.222498 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.222578 titanus.inf.fu-berlin.de.49617 > www.linux.org
11:47:15.233590 titanus.inf.fu-berlin.de.49608 > www.linux.org
11:47:15.237344 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.237472 titanus.inf.fu-berlin.de.49618 > www.linux.org
11:47:15.278850 titanus.inf.fu-berlin.de.49616 > www.linux.org
11:47:15.281037 titanus.inf.fu-berlin.de.49617 > www.linux.org
11:47:15.290554 titanus.inf.fu-berlin.de.49618 > www.linux.org
11:47:15.303033 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.303175 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.417733 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.417745 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.426488 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.430184 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.430194 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.431501 www.linux.org.http > titanus.inf.fu-berlin.de.
```

## Sniffing-Angriffe: Vorgehen

- 3. Schritt – Auswertung des Datenteils
  - Im Beispiel ASCII-Textdarstellung eines Ethernet-Datenpaketes gewählt (Punkte stehen für Steuerzeichen)

```

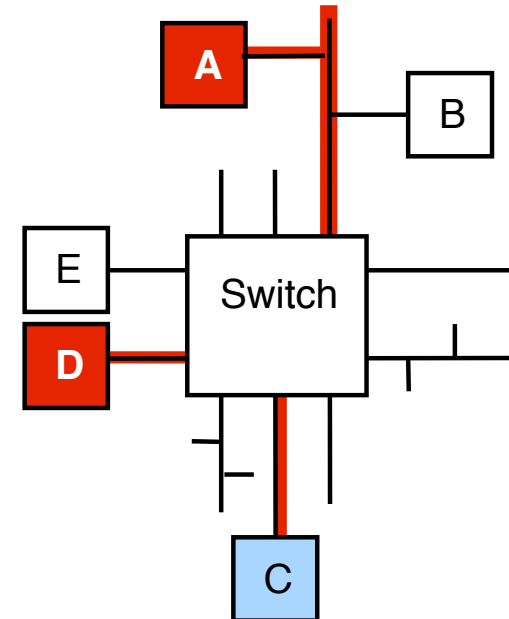
....Ih..OyB..OyB...E...S'@.....QP\..G<..C.H.M../(~.P.....>.*... ..
..E.....w.R$.6..f%A....4.6.f%A.....
.....U.....MailSaveOptions...O.U.....SECUREMAIL..
U.....tmpReview...U.....Form MemoU.....Type..
MemoU.....DeletionPeriod.....>@U.....HoldPeriod..
.....U.....ReturnReceiptS..OnU.....DeliveryReport
--B=U.....Sign..liU.....DefaultMailSaveOptions..lrU.
D.....ReplyToa..U.....Body.....Hallo,.....
.....,.....das ist ein Test f.r unsere Sneaker.....
.....-.....THE MAGIC WORDS ARE FEEBLE GIBBERISH.....
.....Gru.,.....Matthias
Mueller.....U.....ReminderDate..U.....Dele
tionDate..U.....Encrypts..OtU.....$Folders..U.....
....PreparedToSend..O U.....DeliveryPriority..NMU.....
..$KeepPrivate..U.....Subject ..Testmail fuer SniffingU.E.
..6.....SendTo..CN=Andreas Maier/OU=DuD/OU=Datenschutz/O=TUD@TU-Dresd
enU.E.....CopyTo..U.D.....BlindCopyTo..U.E..../.Fr
om..CN=Matthias Mueller/OU=DuD/OU=Datenschutz/O=TUD.EU.....Po
stedDate..}.6..f%AU.....i.....$Signature.....X6..f%A.....O...
.....6...H.....j8..d%.....&...@.....$.
.a%...$.t.%.....O=TUD.....O=TUD.....BV...l.O.BC...BA..0BL..v.NN
P...w...%m...]i.u....;,.ys}.}.4].yl.). ...C...|ohi<'5L.r..B...
BZ%;m<....L...Q])..EN..D..MA..l...So;|.PURSAFO..d.YK.....<>3.....
.#->k.....|.Jj/..R..|.U...ka..Ofz.....@@

```

## Spoofing-Angriffe: Funktionsweise (Ethernet)

Rechner **A** und **D** kommunizieren miteinander:

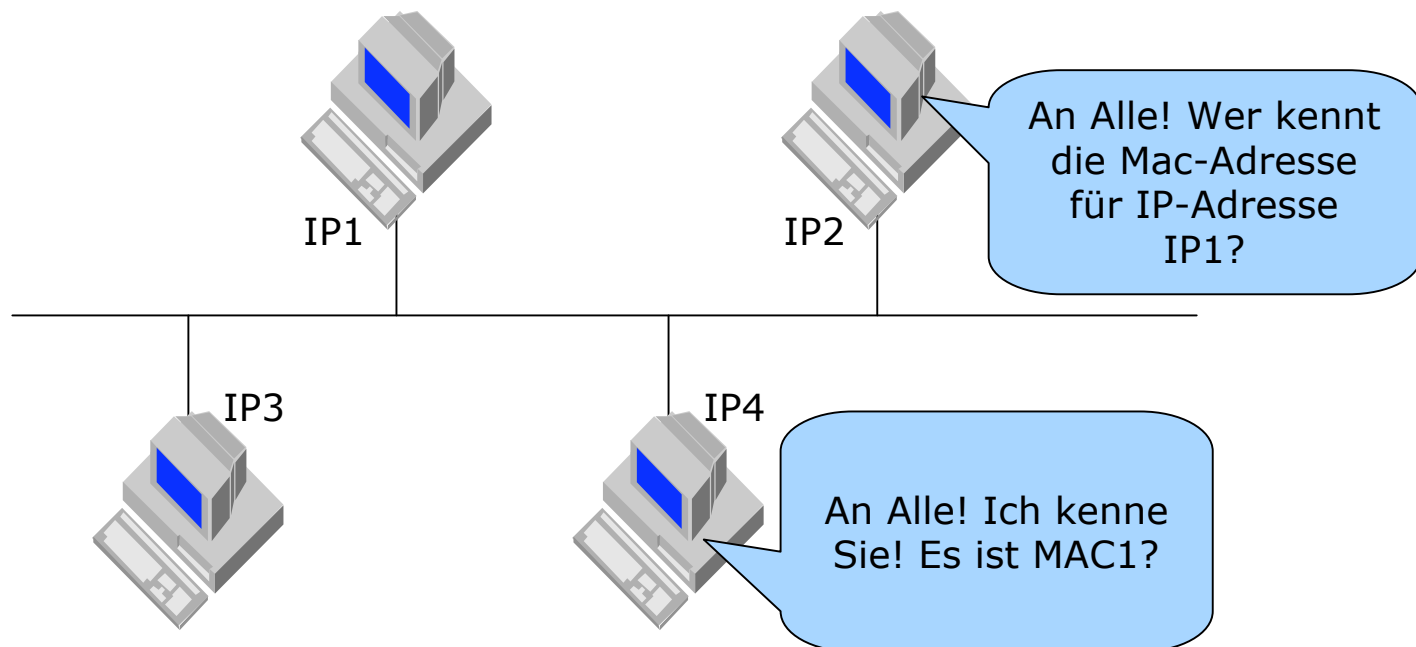
b) im Switched Ethernet



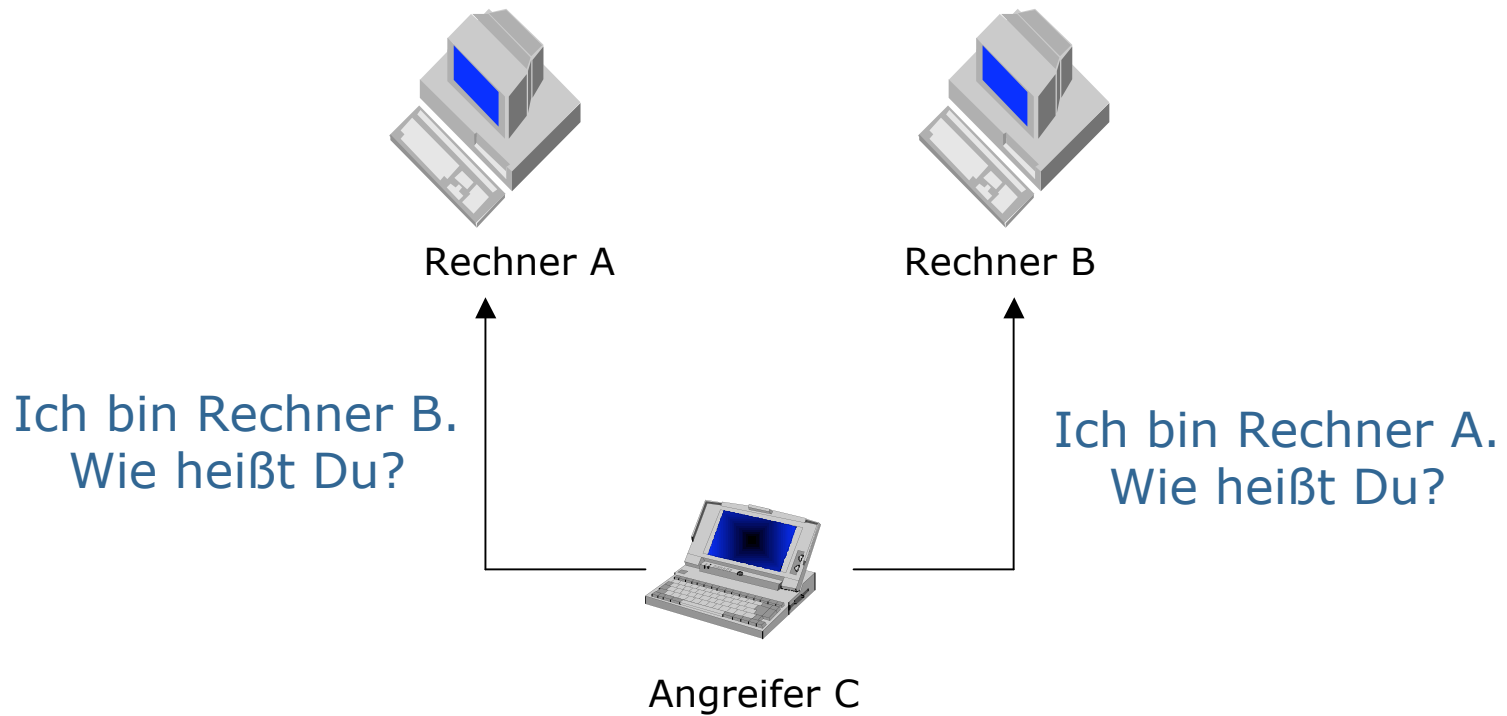
C greift an

## ARP: Address Resolution Protocol

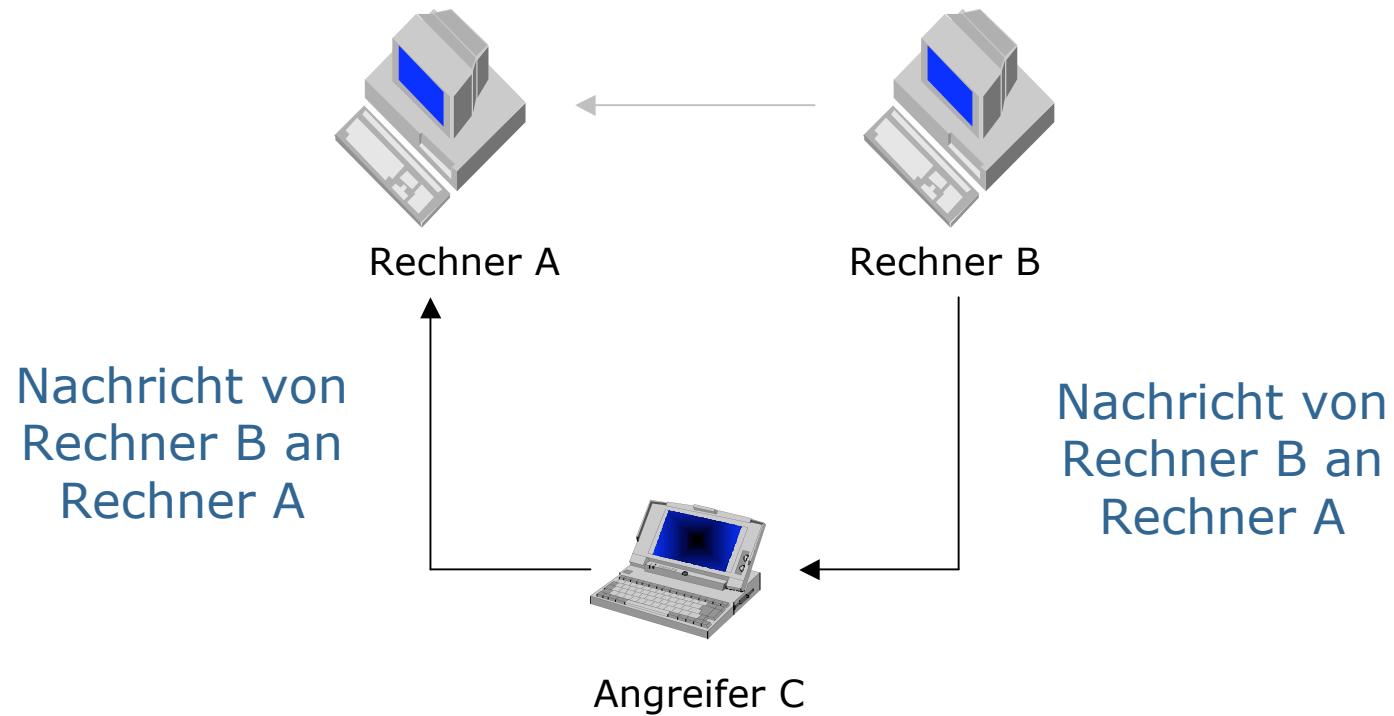
- ARP-Anfrage
  - Anfrage wird an das gesamte lokale Netz gestellt (Broadcast)
  - Mitteilen der eigenen Adresse(n) in der Anfrage
- ARP-Antwort
  - Jeder Rechner, der die Zuordnung kennt, kann antworten



## > ARP-Spoofing



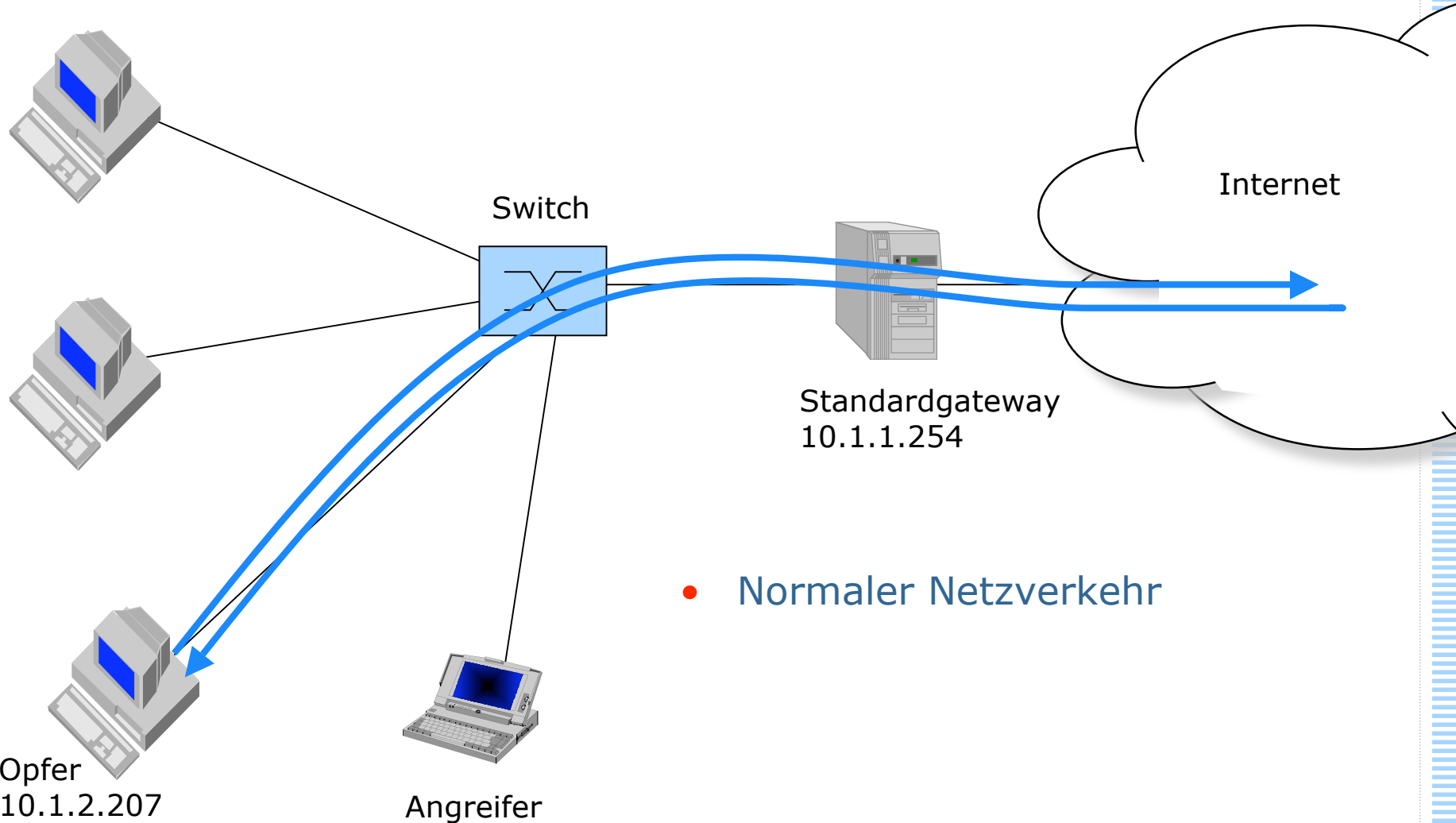
## &gt;&gt; ARP-Spoofing





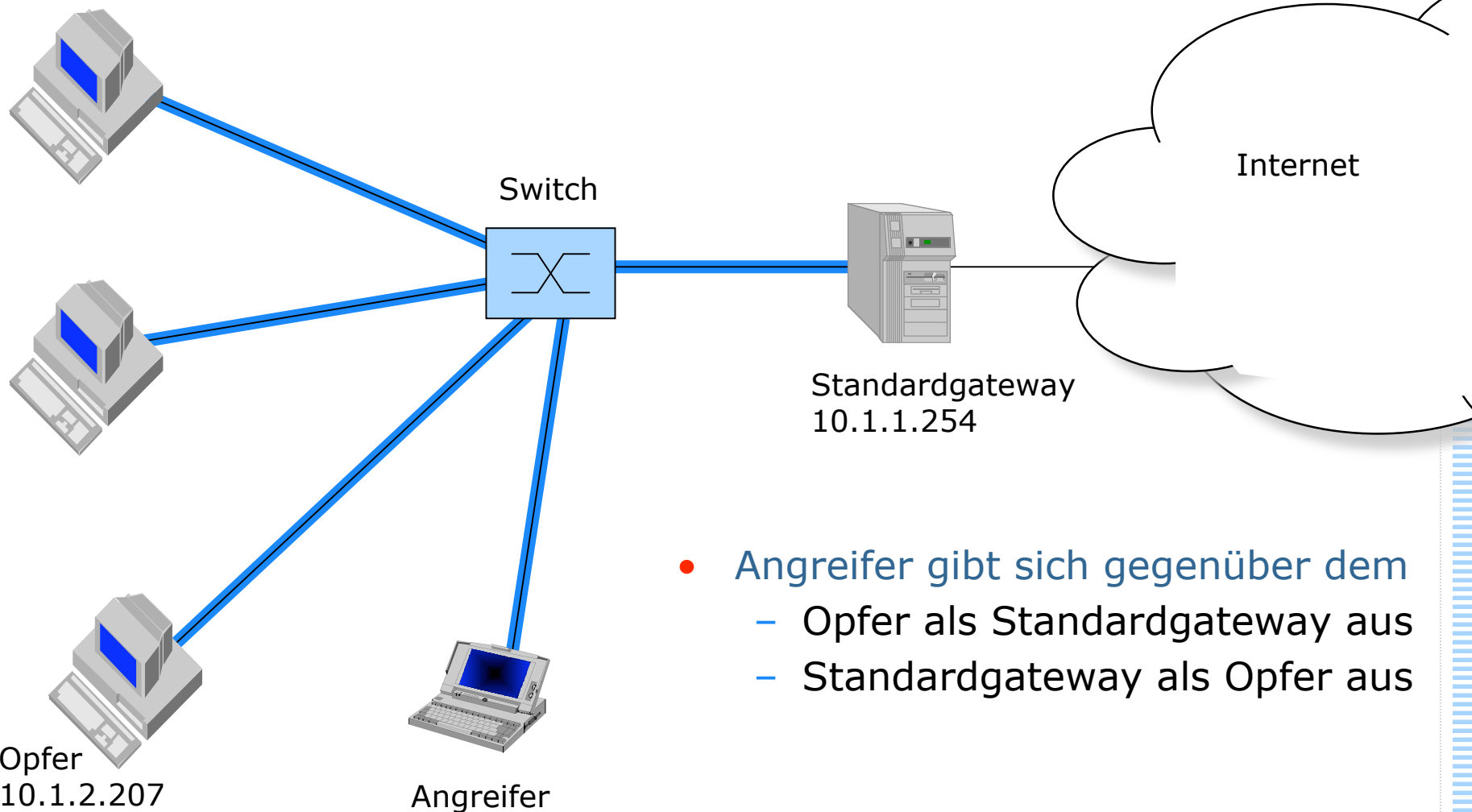
# Netzwerktopologie ARP-Spoofing-Demonstration

Weitere Rechner im Subnetz  
10.1.0.0/255.255.252.0



## ARP-Spoofing: Vorbereitung

Weitere Rechner im Subnetz  
10.1.0.0/255.255.252.0



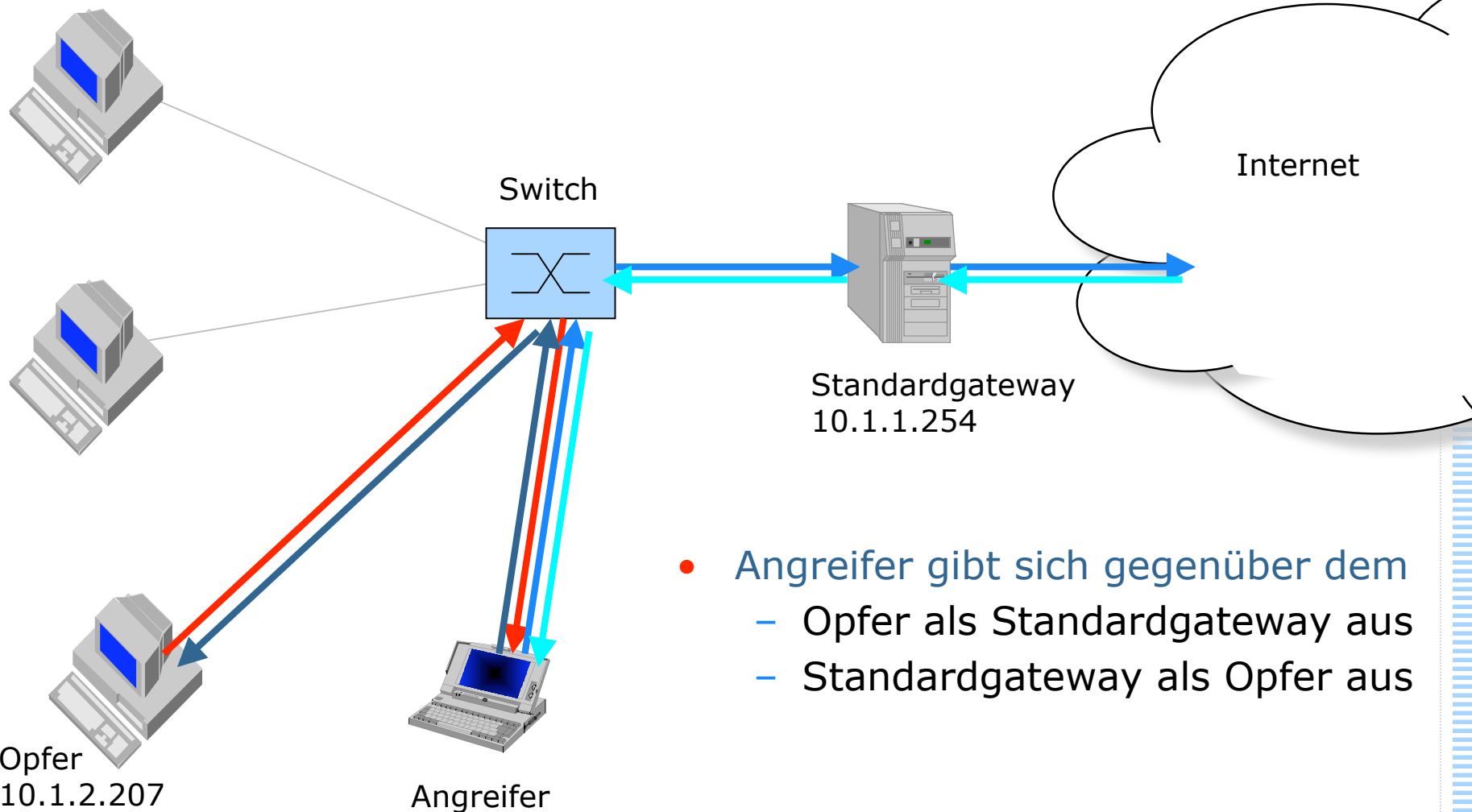
- Angreifer gibt sich gegenüber dem
  - Opfer als Standardgateway aus
  - Standardgateway als Opfer aus

Opfer  
10.1.2.207

Angreifer

# ARP-Spoofing: Opfer will IP-Paket ins Internet senden

Weitere Rechner im Subnetz  
10.1.0.0/255.255.252.0

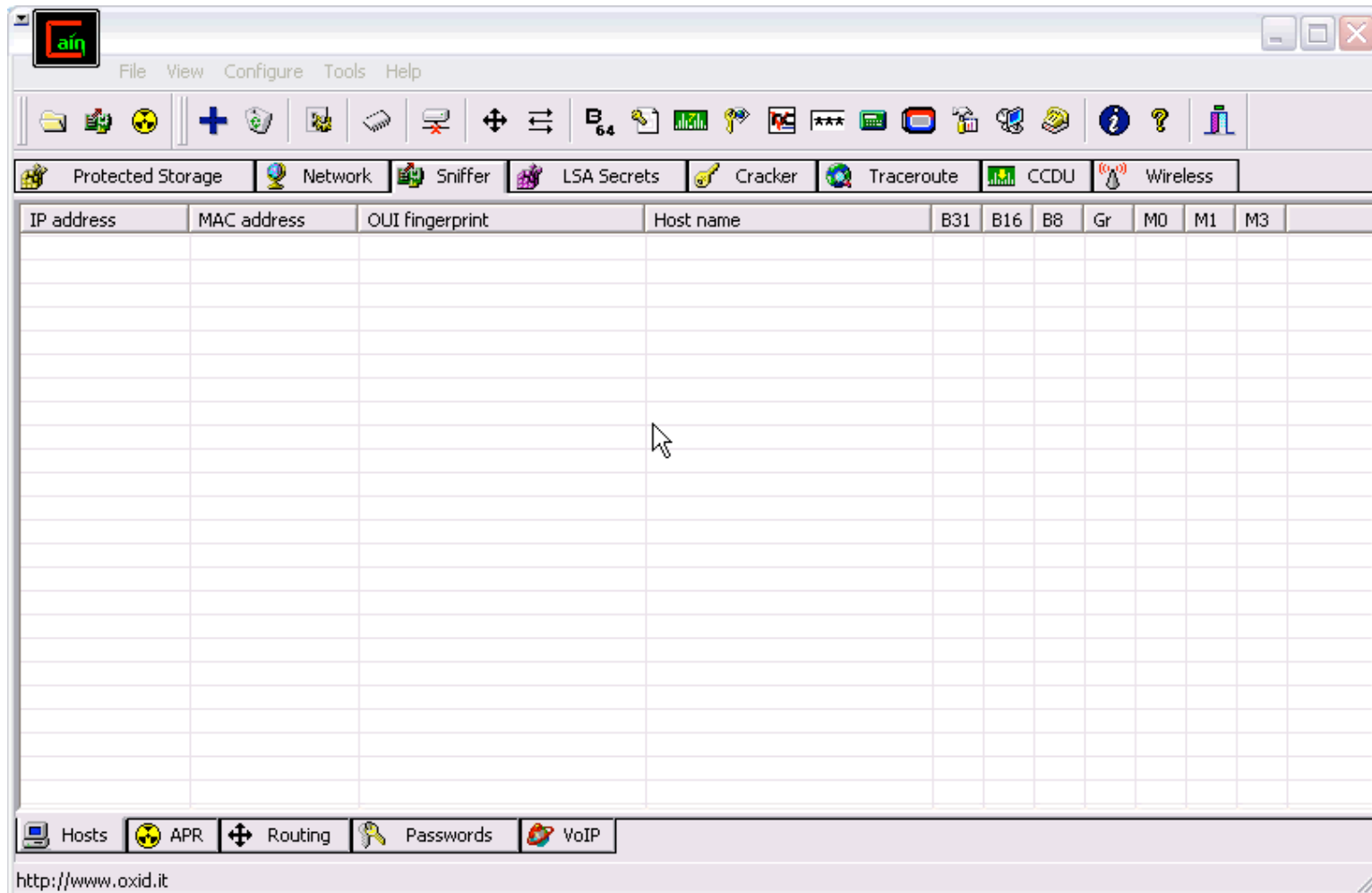


- Angreifer gibt sich gegenüber dem
  - Opfer als Standardgateway aus
  - Standardgateway als Opfer aus

## ARP-Spoofing

- Angreifer
  - empfängt den gesamten Netzwerkverkehr
    - vom Opfer zum Internet
    - vom Internet zum Opfer
  - kann diese Datenpakete beliebig manipulieren
- Demonstration:
  - Windows Tool „Cain & Abel“
    - <http://www.oxid.it/cain.html>
  - ARP-Spoofing:
    - Opfer: 10.1.2.207
    - Standardgateway: 10.1.1.254
  - DNS-Spoofing:
    - Umleitung von [www.bsi.de](http://www.bsi.de) nach [jap.inf.tu-dresden.de](http://jap.inf.tu-dresden.de)

# Rechner im Netzwerk identifizieren



# Auswahl der Rechner für das ARP-Spoofing

The screenshot shows the main window of the Cain & Abel network analysis tool. The 'Sniffer' tab is selected in the top toolbar. Below the toolbar, a table displays the following data:

IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
10.1.1.1	0040CA190C2C	FIRST INTERNAT'L COMPUTE...								
10.1.1.2	0040CA18AAA6	FIRST INTERNAT'L COMPUTE...								
10.1.1.254	00E0B0E2906B	CISCO SYSTEMS, INC.								
10.1.2.206	000A95E8B4FC	Apple Computer, Inc.								
10.1.2.207	00D059D78A2F	AMBIT MICROSYSTEMS CORP.								
10.1.2.241	000D56C93866	Dell PCBA Test								
10.1.2.248	0001E697FD91	Hewlett-Packard Company								

The bottom status bar indicates 'Lost packets: 0%'.

# Einrichten des DNS-Spoofing

The screenshot shows the aircrack-ng application window. The left sidebar displays a tree structure under 'APR' with sub-items: APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), and APR-RDP (0). The main window is divided into two sections. The top section is titled 'Configuration / Routed Packets' and contains a table with the following data:

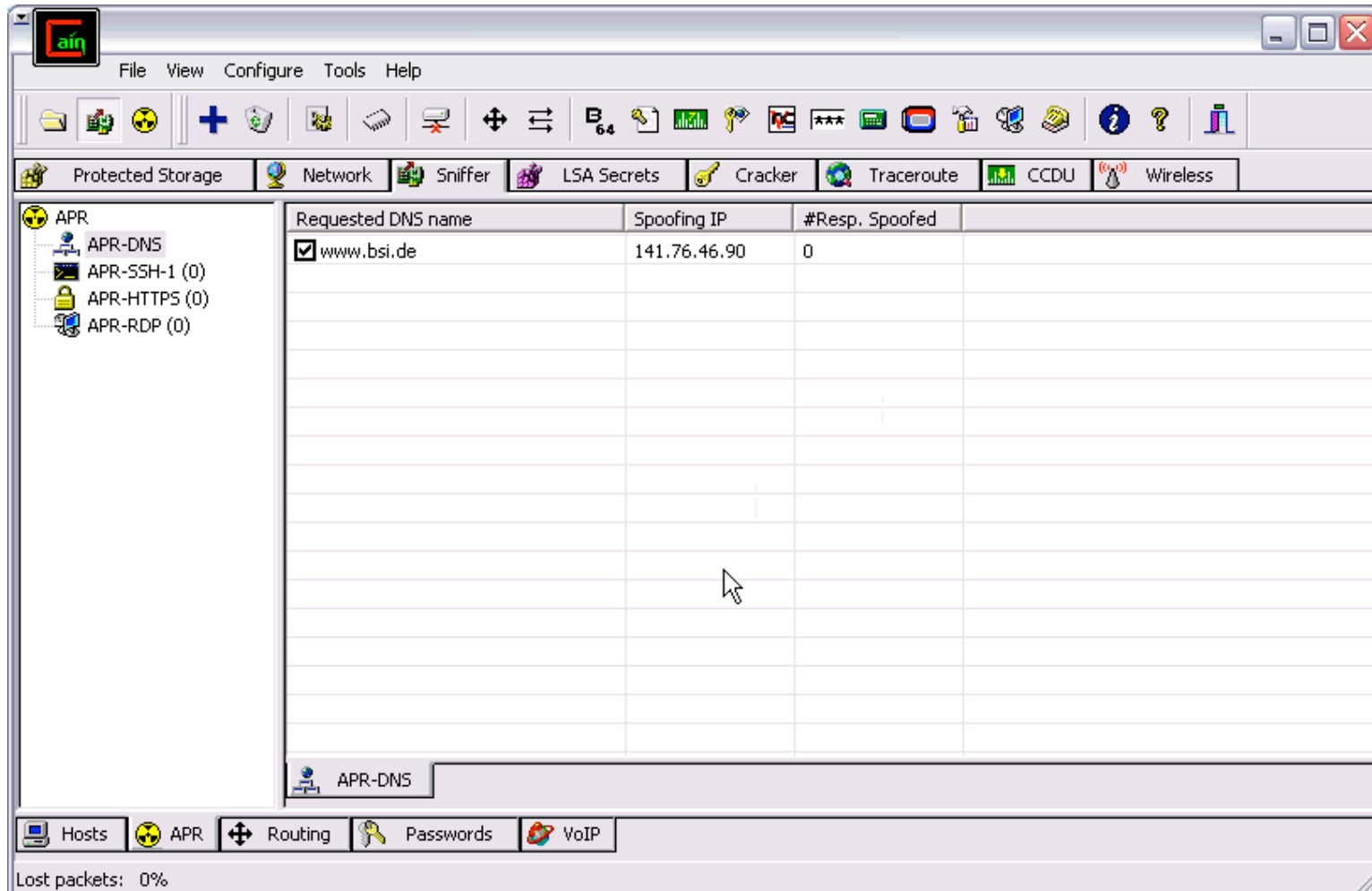
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.1.2.207	00D059D78A2F			00E0B0E2906B	10.1.1.254

The bottom section is titled 'Configuration / Routed Packets' and contains a table with the following data:

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

The bottom status bar shows 'Lost packets: 0%'.

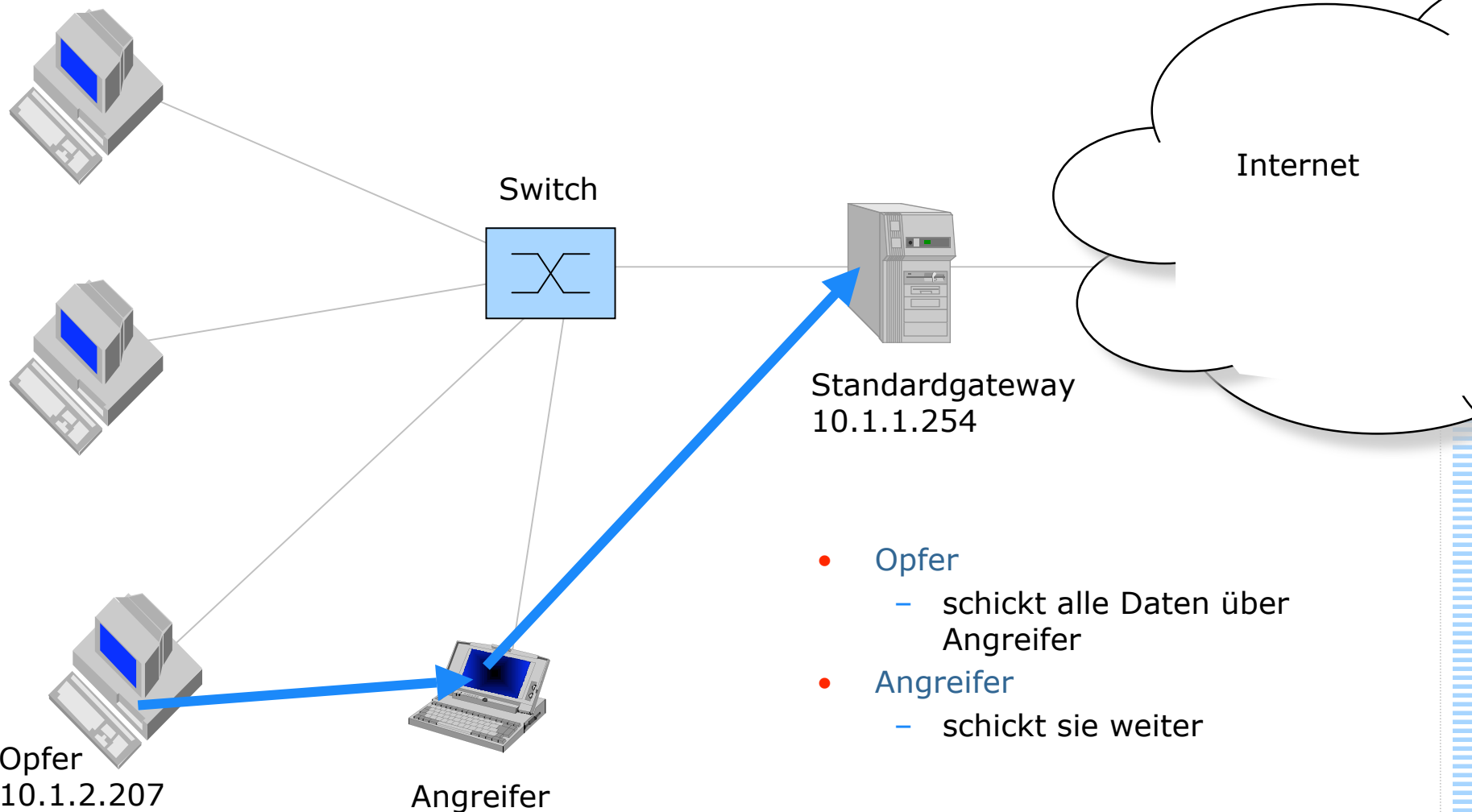
## Start des ARP- und DNS-Spoofings





## Erreichte Situation

Weitere Rechner im Subnetz  
10.1.0.0/255.255.252.0



Opfer  
10.1.2.207


Angreifer

# Sicht des Opfers

Lehrveranstaltungsangebote - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://www-sec.uni-regensburg.de/teaching/

 **IT-Sicherheitsmanagement** Lehrstuhl Management der Informationssicherheit

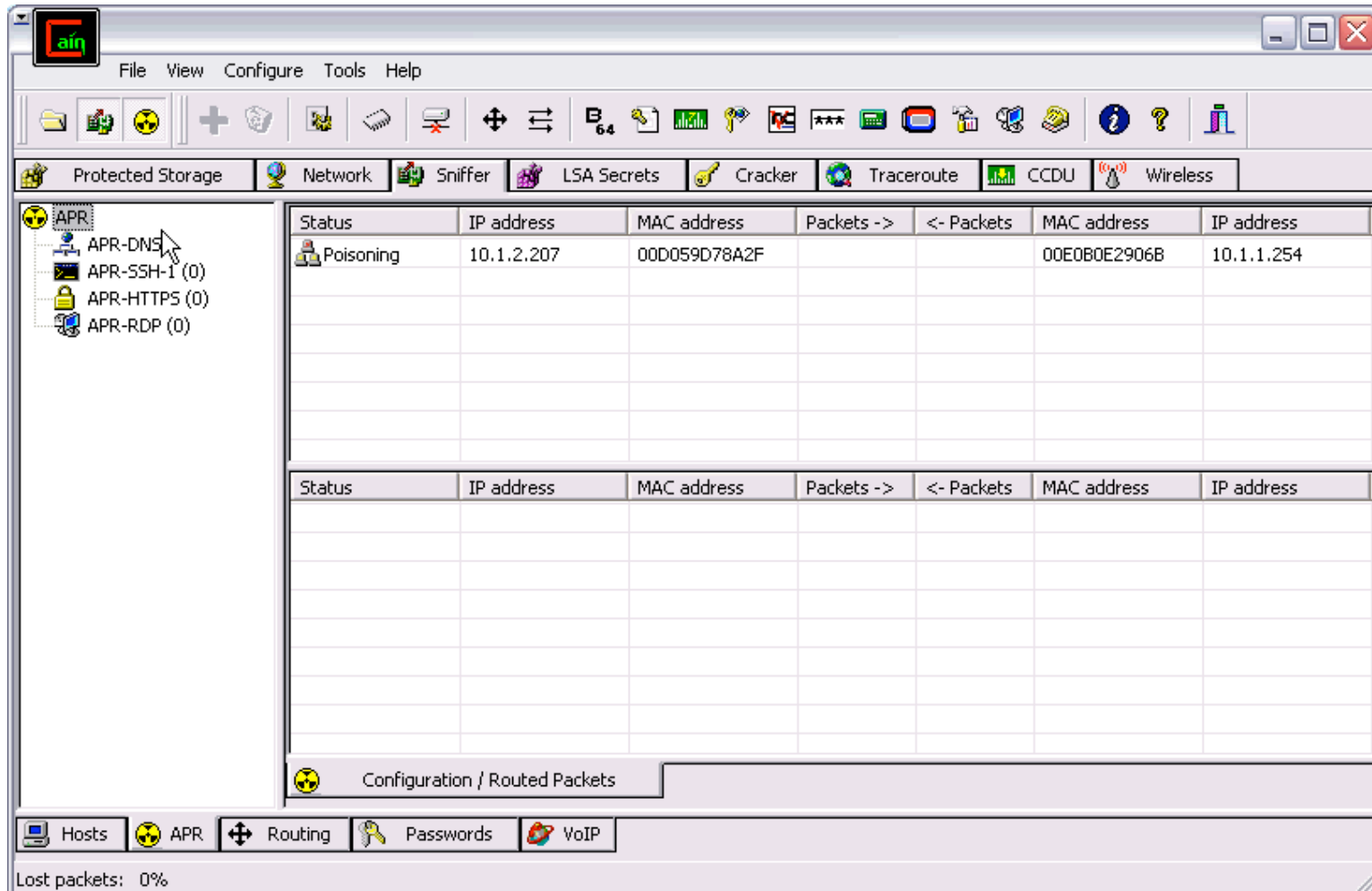
Universität Regensburg > Wirtschaftswissenschaften > Wirtschaftsinformatik

**Lehrveranstaltungsangebote**

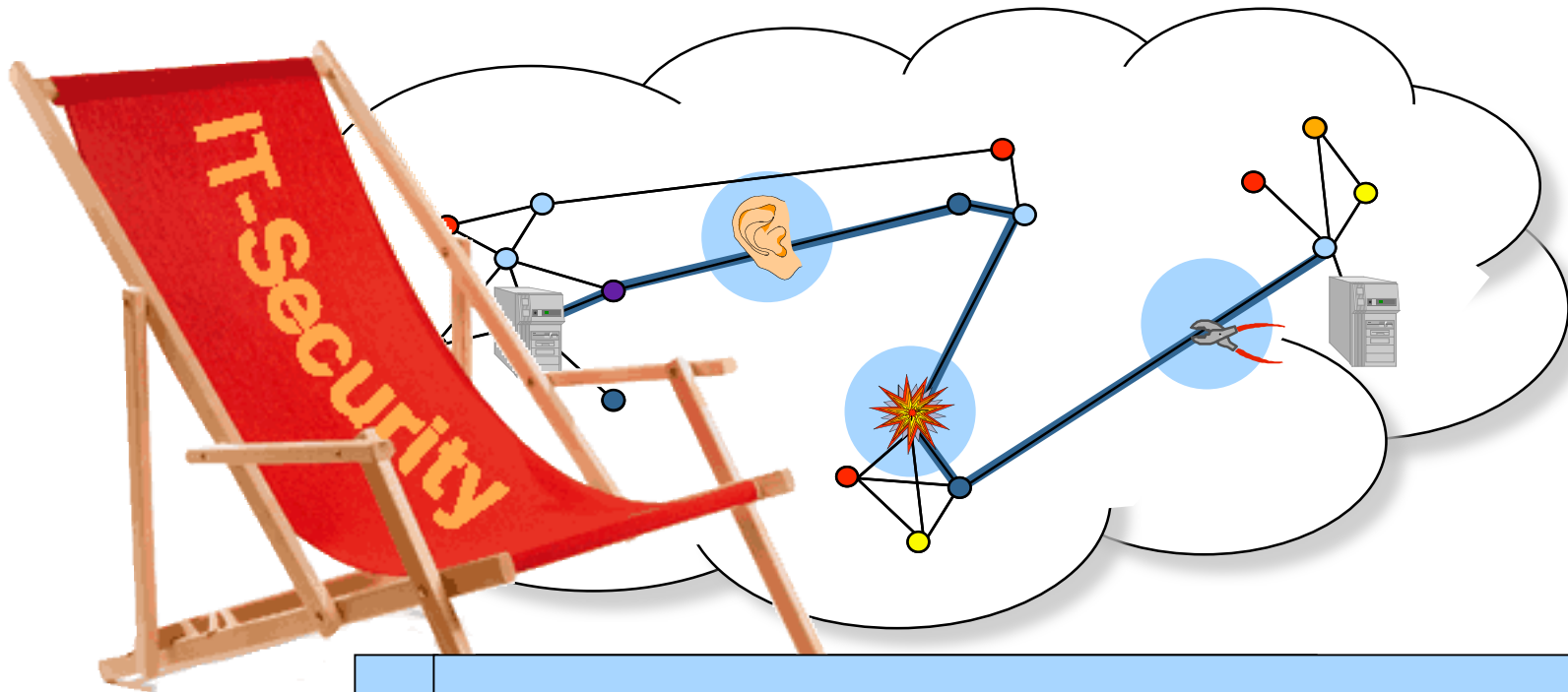
Lehrveranstaltungsangebote des Lehrstuhls | Vorlesungsfolien in der VUR | Themen für Diplomarbeiten | Schwerpunkt Informationssicherheit | Modellstudienplan Informationssicherheit

Wintersemester	SWS	Art
VL Informatik III (Algorithmen und Datenstrukturen)	2/2	Grundstudium
VL Allgemeine Wirtschaftsinformatik (Datenkommunikation)	2/1	Hauptstudium
Seminar IT-Sicherheit	2	Hauptstudium
Diplomanden- und Doktorandenseminar	2	Hauptstudium
VL Sicherheitsmanagement	2/1	Schwerpunkt Informationssicherheit
VL Sicherheit mobiler Systeme	2/-	Schwerpunkt Informationssicherheit
VL Praxis der IT-Sicherheit (bedarfsweise)	1/3	Schwerpunkt Informationssicherheit
<b>Sommersemester</b>		
VL Informatik IV (Objektorientierte Programmierung)	2/1	Grundstudium
Projektseminar Informationssicherheit	2	Hauptstudium
Diplomanden- und Doktorandenseminar	2	Hauptstudium
VL IT-Sicherheit	2/2	Schwerpunkt Informationssicherheit

## Sicht des Angreifers



# Abwehr



- V: Offene Systeme, Diversität, Berechtigungskonzepte
- P: Kryptographie, insb. PKI
- S: Kryptographie, insb. Verschlüsselung